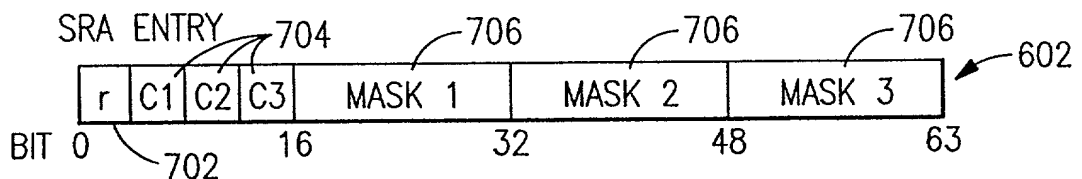


**FIG.5**

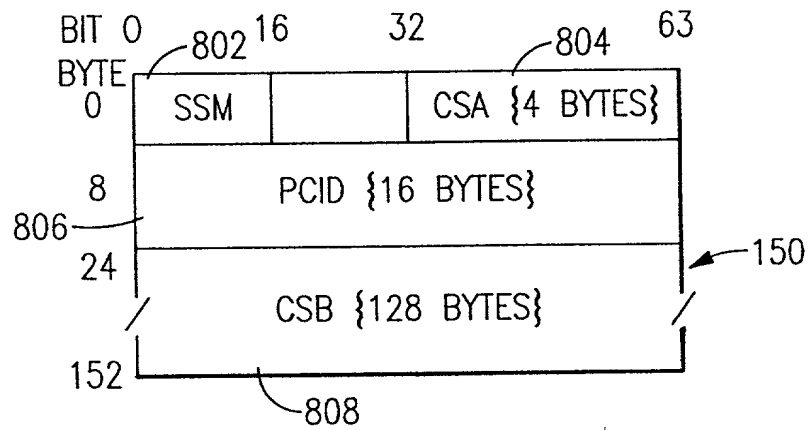
BYTE SIGNATURE-REQUIREMENT ARRAY (SRA) 156

0	ENTRY 0, FOR LOAD AUTHORIZATION PUBLIC MODULUS (LAP)	602
8	ENTRY 1, FOR LOAD PKSC CONTROL BLOCK (LCB)	602
16	ENTRY 2, FOR ZEROIZE DOMAIN (ZD)	602
24	ENTRY 3, FOR LOAD ENVIRONMENT-CONTROL MASK (LEC)	
32	ENTRY 4, FOR EXTRACT AND ENCRYPT MASTER KEY (XEM)	
40	ENTRY 5, FOR LOAD KEY PART (LKP)	
48	ENTRY 6, FOR EXTRACT AND ENCRYPT SMK OR RMK (XES OR XER)	
56	ENTRY 7, FOR LOAD AND COMBINE SMK OR RMK (LCS OR LCR)	
64	ENTRY 8, FOR REENCIPHER TO SMK OR RMK (RTS OR RTR)	
72	ENTRY 9, FOR REENCIPHER FROM SMK OR RMK (RFS OR RFR)	

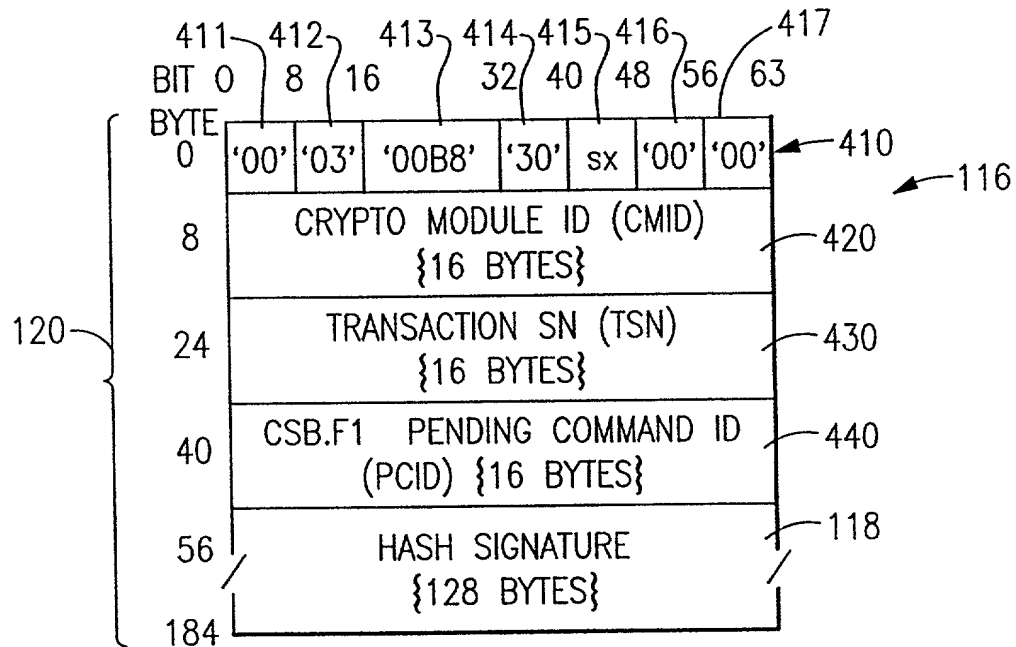
**FIG.6**



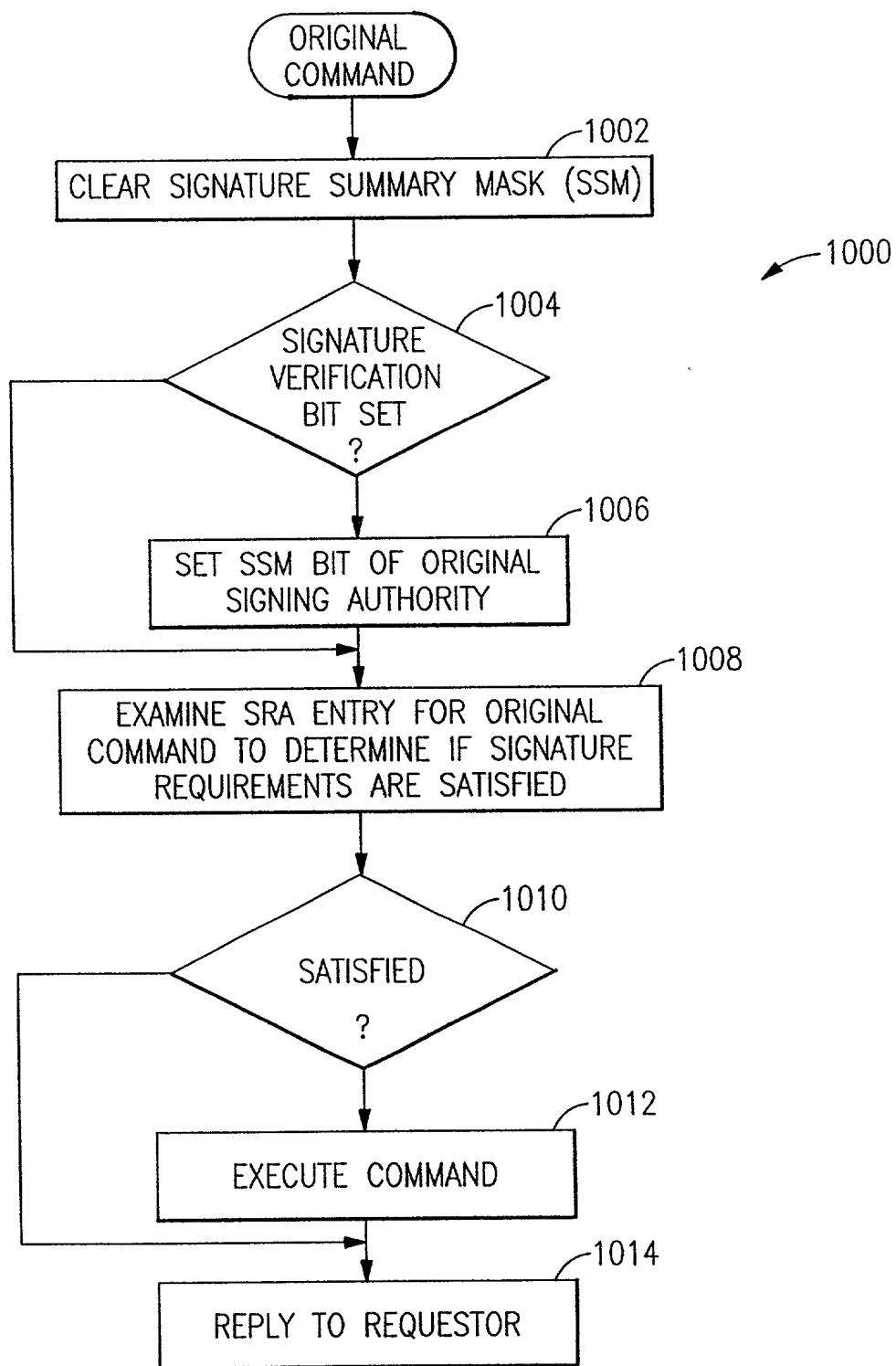
**FIG.7**



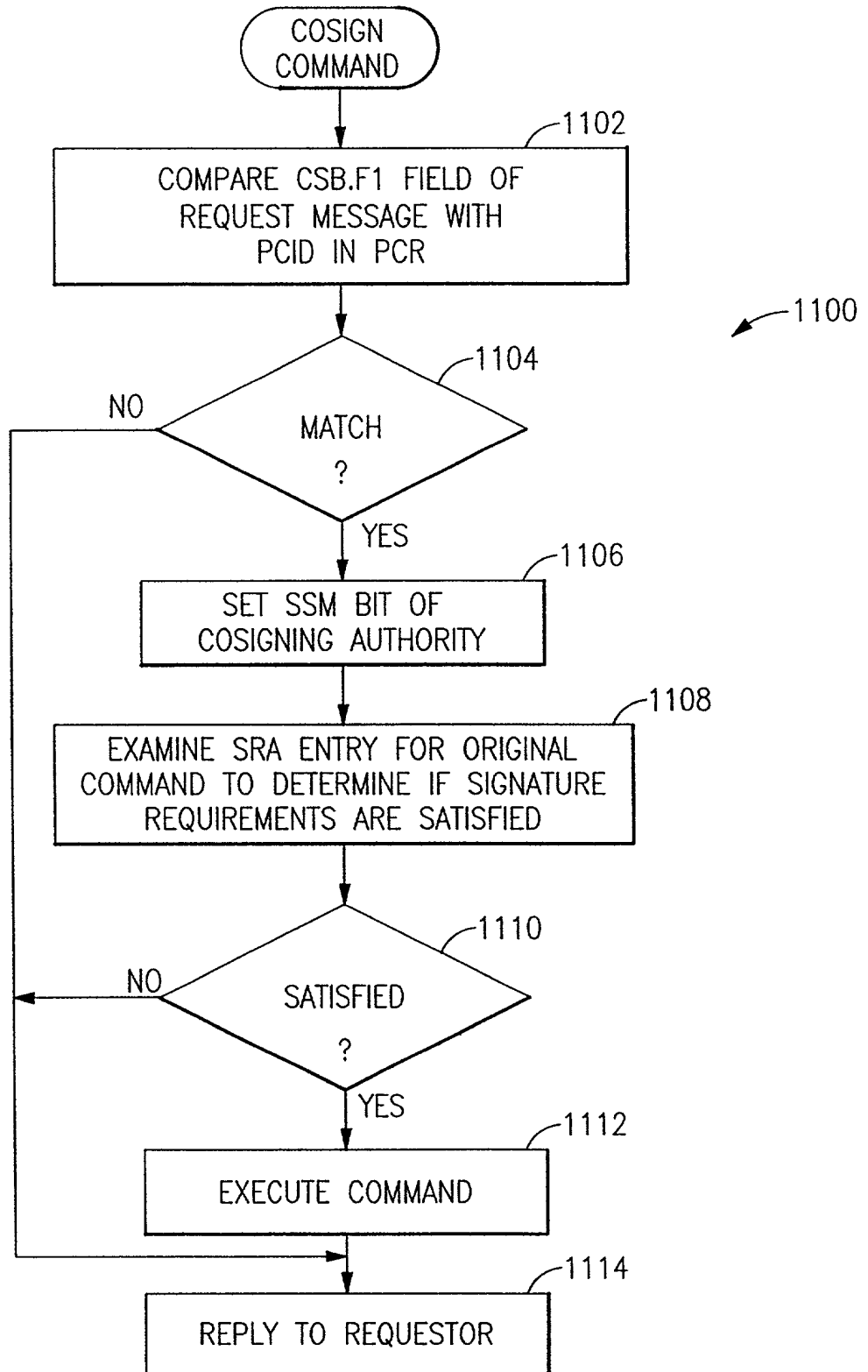
**FIG. 8**



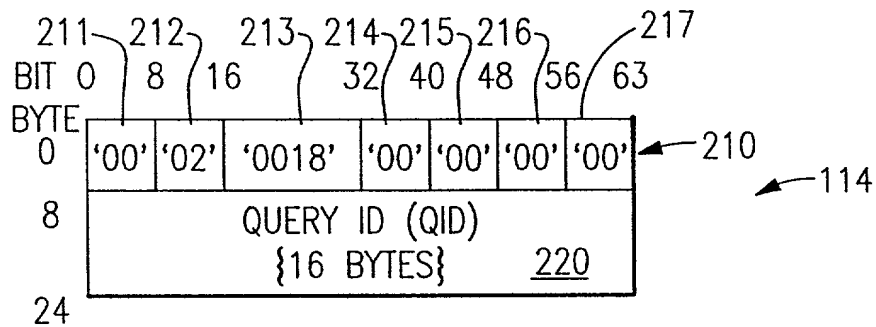
**FIG. 9**



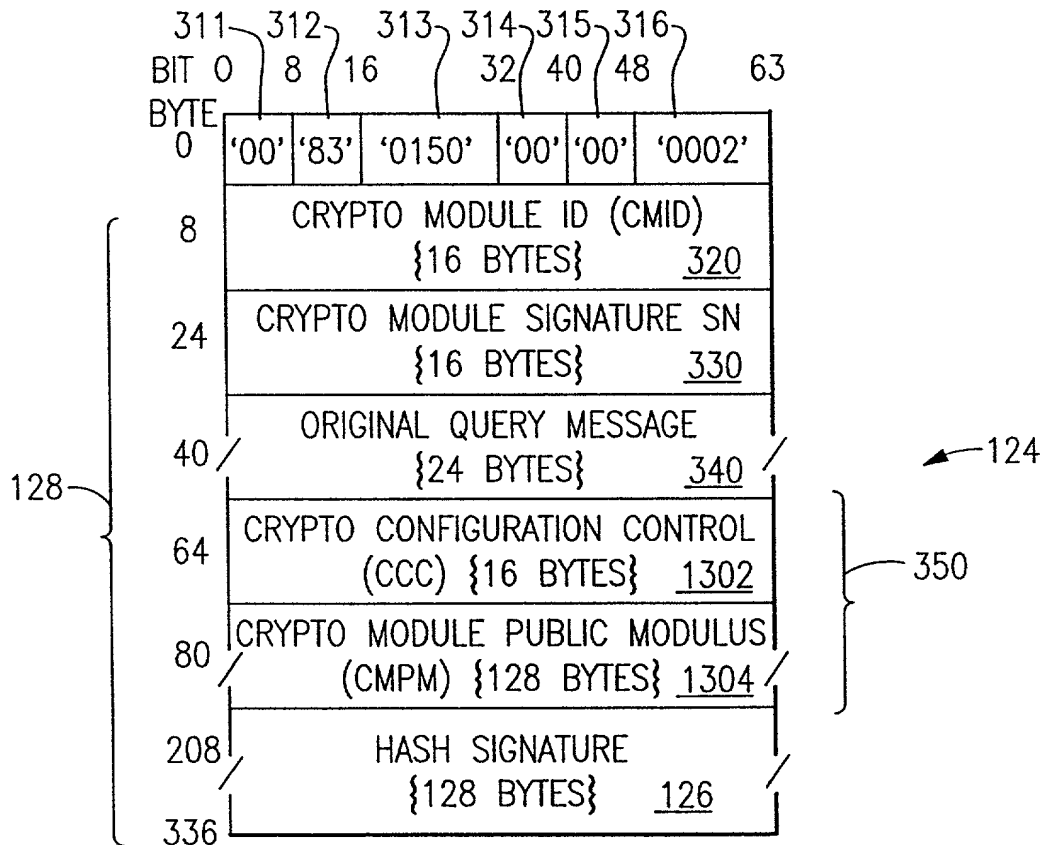
**FIG.10**



**FIG.11**



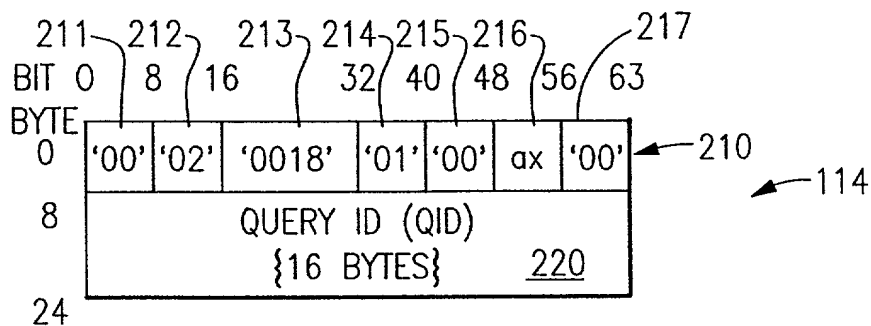
**FIG.12**



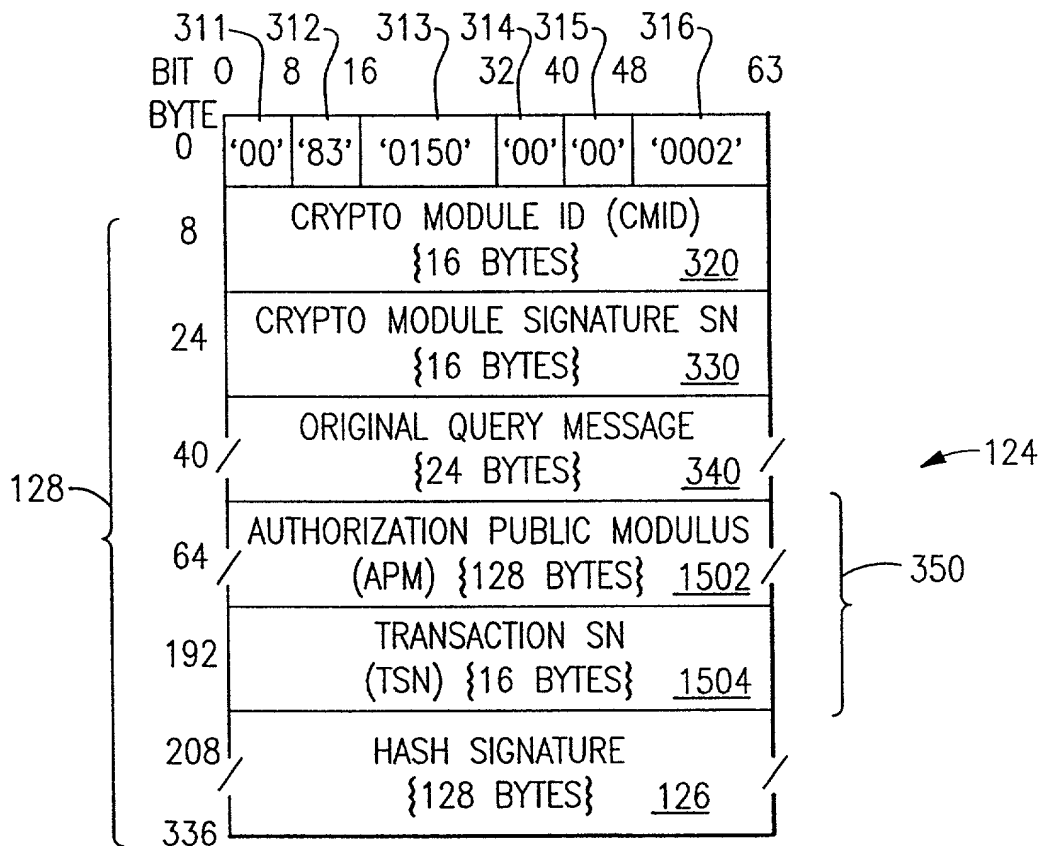
**FIG.13**

00000000 558844260

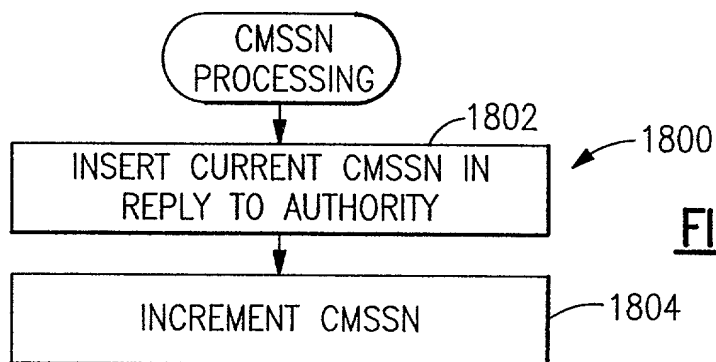
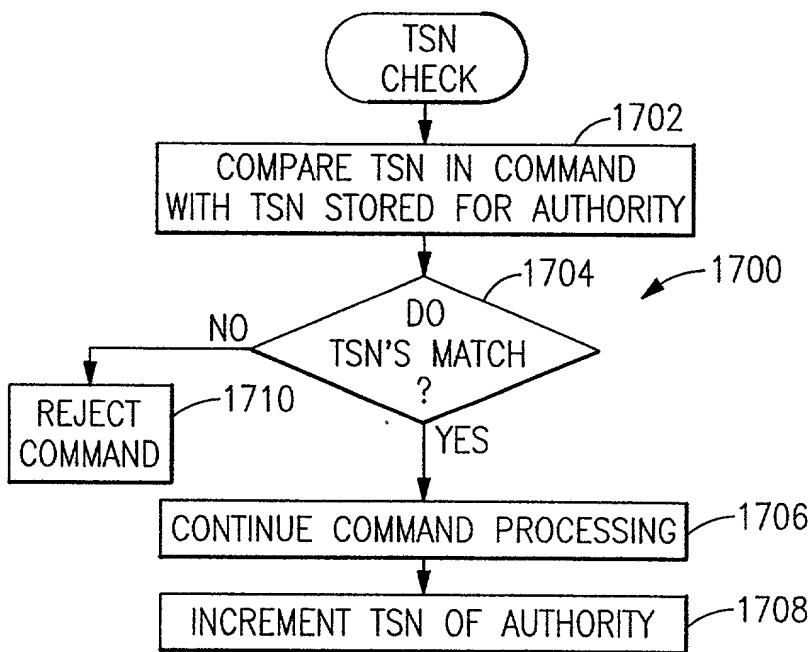
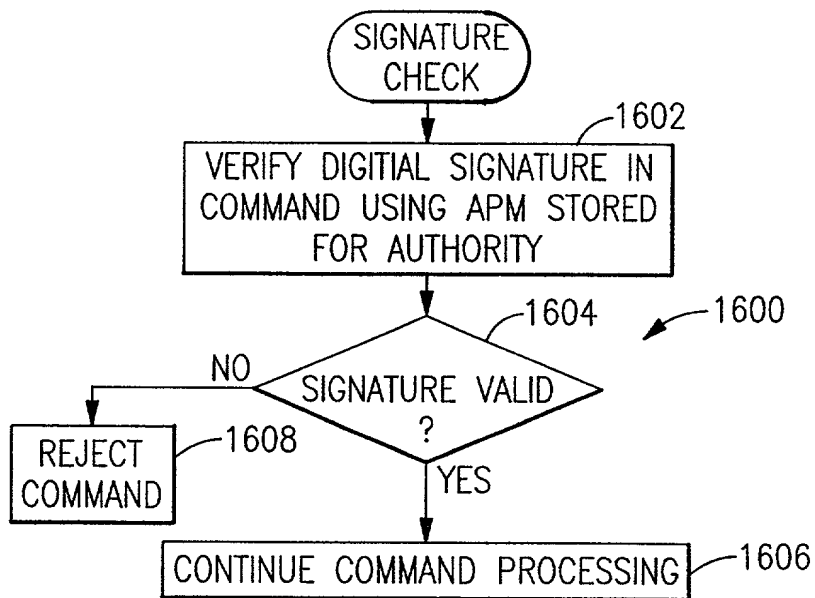




**FIG. 14**



**FIG. 15**



09748899-122700